

Exhibit FF

UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK

-----	X:
	:
SIMO HOLDINGS INC.,	:
	:
Plaintiff,	: No. 1:18-cv-05427 (JSR)
	:
-against-	:
	:
HONG KONG UCLOUDLINK NETWORK	:
TECHNOLOGY LIMITED and	:
UCLOUDLINK (AMERICA), LTD.,	:
	:
Defendants.	X

INVALIDITY REPORT OF MARTIN J. FEUERSTEIN

TABLE OF CONTENTS

I. INTRODUCTION	1
II. BACKGROUND AND QUALIFICATIONS	2
III. DOCUMENTS AND OTHER MATERIALS RELIED UPON	4
IV. RELEVANT LAW AND LEGAL STANDARDS	5
A. Date of Invention	5
B. Anticipation	5
C. Obviousness	6
D. Enablement	8
E. Standard of Proof	9
V. LEVEL OF ORDINARY SKILL IN THE ART	9
VI. OVERVIEW OF THE '689 PATENT	10
A. Summary of Technology Discussed in the '689 Patent	10
B. Prosecution History for the '689 Patent	14
VII. CLAIM CONSTRUCTION	15
VIII. THE PRIOR ART	16
A. Overview of <i>Andreini</i>	16
B. Overview of <i>Patarkazishvili</i>	17
C. Overview of <i>Walton</i>	19
D. Overview of <i>Shi</i>	21
E. Overview of <i>Kasper</i>	21
IX. INVALIDITY OVER THE PRIOR ART	23
A. <i>Andreini</i> Anticipates, or Alternatively <i>Andreini</i> in View of <i>Walton</i> Renders Obvious, Claims 8 and 11-13	23
1. Claim 8	23
2. Claim 11	38
3. Claim 12	39
4. Claim 13	41
B. <i>Andreini</i> in View of <i>Shi</i> or (<i>Shi</i> and <i>Walton</i>) Renders Claim 14 obvious	43
C. <i>Patarkazishvili</i> Anticipates, or Alternatively <i>Patarkazishvili</i> in View of <i>Walton</i> Renders Obvious, Claims 8 and 11-13	46
1. Claim 8	47
2. Claim 11	60
3. Claim 12	62

4.	Claim 13.....	63
D.	<i>Patarkazishvili</i> in View of <i>Shi</i> and <i>Walton</i> Renders Claim 14 Obvious.....	65
E.	<i>Kasper</i> in view of <i>Walton</i> Renders Claims 8 and 11-13 Obvious.....	67
1.	Claim 8.....	67
2.	Claim 11.....	76
3.	Claim 12.....	77
4.	Claim 13.....	78
X.	CLAIM 8 IS INVALID UNDER 35 U.S.C. 112	79
XI.	CONCLUSION	83

15. For more information on my educational and professional background relating to mobile telecommunication systems, networks and devices, and related technologies, refer to my curriculum vitae, attached in Appendix 1.

16. Based on my technical experience in the field of wireless communications, including that summarized above and described in greater detail in my curriculum vitae, I consider myself to be an expert in the field of mobile telecommunication systems and devices.

III. DOCUMENTS AND OTHER MATERIALS RELIED UPON

17. In the course of preparing this Report, I reviewed the materials listed herein, including the '689 patent and its original prosecution history before the U.S. Patent and Trademark Office:

18. Appendix 2: U.S. Publication No. 2004/0072591 to Andreini; Published: April 15, 2004.

19. Appendix 3: U.S. Patent Publication No. 2009/0225736 to Patarkazishvili; Filed May 17, 2009 and published September 10, 2009; a continuation of PCT/IL2007/001478 filed on November 29, 2007, which claims priority to Provisional Application No. 60/867,826 filed on November 30, 2006.

20. Appendix 4: PCT International Application Publication No. WO 2006/094564 to Walton; Filed: Nov. 9, 2005; Published: Sept. 14, 2006.

21. Appendix 5: U.S. Patent Application Publication No. US 2009/0163175 to Shi et al.; Filed: Dec. 24, 2007; Published: Jun. 25, 2009.

22. Appendix 6: Diploma thesis entitled "Virtualisation of a SIM-Card using Trusted Computing" by Kasper; Publicly available since April 30, 2007.

23. Appendix 7: 3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; Security aspects 02.09 v8.1.0; Published: June 2006.
24. Appendix 8: European Telecommunications Standards Institute (ETSI) GSM Technical Specification, GSM 04.08, Version 5.3.0; Published: July 1996.
25. Appendix 9: ISO/IEC 7816-4:2005 Identification cards -- Integrated circuit cards -- Part 4: Organization, security and commands for interchange; Published: 2005.
26. Appendix 10: The Court's Claim Construction Order dated November 1, 2018.
27. Appendix 11: The Court's Claim Construction Opinion Dated November 9, 2018.

IV. RELEVANT LAW AND LEGAL STANDARDS

A. Date of Invention

28. The '689 Patent was issued from Application Serial No. 13/372,345 ("the '345 application") filed on February 13, 2012 as continuation of Application Serial No. 12/039,646 ("the '646 application"), filed on February 28, 2008. I have been told to assume that February 28, 2008 is the earliest purported priority date for the asserted claims. As otherwise noted, I will use the earliest priority date as the date of invention for purposes of my analysis.

B. Anticipation

29. I am informed and understand that a patent claim is invalid under 35 U.S.C. § 102² if each and every element of the claim is disclosed either expressly or inherently in a single prior art reference.

² I have been informed and understand that the references in this Report to 35 U.S.C. §§ 102, 103, and 112 refer to their respective pre-AIA versions since the '689 patent was filed before March 16, 2013. *See* America Invents Act, P.L. 112-29 (Sept. 16, 2011) at § 3(n) (amendments to 35 U.S.C. §§ 102, 103, and 112 take effect and apply to applications that contain or contained at any time a claim with an effective filing date on or after March 16, 2013).

D. Overview of *Shi*

71. U.S. Patent Application Publication No. 2009/0163175 to Shi (“*Shi*”) was filed on December 24, 2007 and published on June 25, 2009. *Shi* was filed before the priority date of the ’689 patent, and thus qualifies as prior art under 35 U.S.C. § 102(e).

72. *Shi* discloses allowing cell phone users to store their SIM card data (and other personal information) on a remote database. If the user loses his phone (and SIM card), the data from the database can be moved to a new phone and used to connect to a cellular network as if the original SIM card were present. *Shi* at ¶ 31. As part of request for such service, the user must send authentication credential, such as user account name and password, to the remote VSIM server. *Id.* at ¶ 33.

E. Overview of *Kasper*

73. Diploma thesis, entitled “Virtualisation of a SIM-Card using Trusted Computing” submitted by Michael Kasper (“*Kasper*”) on April 30, 2007 to Private Fernfachhochschule Darmstadt, Department of Computer Science, was published in 2007, and thus qualifies as prior art under 35 U.S.C. § 102(a).

74. Although *Kasper* does not tackle the international roaming issue, it introduces a detailed subscriber authentication solution for virtual SIM prior to the ’689 Patent, which is exactly what the applicant claimed *Walton* lacks compared with the ’689 Patent during prosecution. Such virtual SIM technology is the basis of the roaming solution proposed by the ’689 Patent and facilitates the authentication process with a local network carrier in order to enable the roaming solution.

75. Asserted independent claim 8 of the ’689 patent covers relaying of authentication request and authentication information between local network carriers and remote administration

76. More specifically, the authentication request (authentication message RAND) and authentication information (response message SRES) in *Kasper* is consistent with specification of the '689 Patent. '689 Patent at 11:53-61. In *Kasper*, the mobile device initiates an authentication process with a network operator by “relay[ing] IMSI_i” to the network operator. *Kasper* at page 59. The network then “replies” to the mobile device with an authentication request in the form of “authentication challenge RAND_i.” *Id.* The authentication request is then “passed to” a relevant function of the Mobile Trusted Platform in order to derive an authentication information in the form of “challenge response message SRES*.” *Id.* The server “sends” the authentication information to the mobile terminal, which will “relay” it to the network operator. *Id.* The mobile device is subsequently “authenticated” by the network operator and obtains “access in mobile cellular networks” as if it is a local wireless device. *Id.* at page 59 and 57.

IX. INVALIDITY OVER THE PRIOR ART

A. *Andreini* Anticipates, or Alternatively *Andreini* in View of *Walton* Renders Obvious, Claims 8 and 11-13

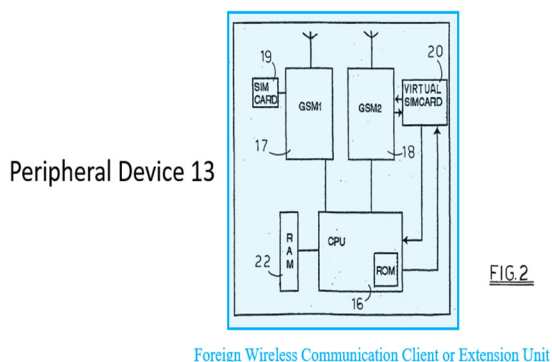
77. As explained below, it is in my opinion that *Andreini* discloses each and every element of claims 8 and 11-13, either expressly or inherently, and thus anticipates these claims. Or alternatively, to the extent of the preamble of independent claim 8 is limiting, *Andreini* in view of *Walton* discloses, suggests, or teaches all elements of claims 8 and 11-13, and thus renders these claims obvious.

1. Claim 8

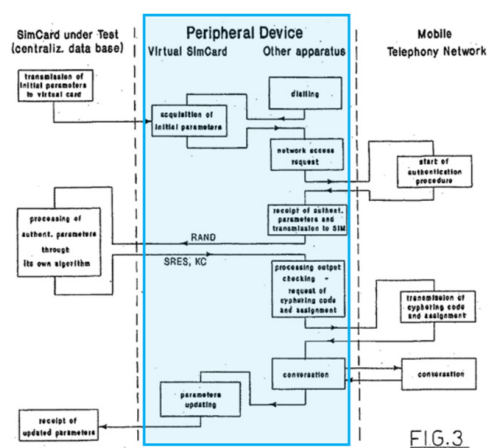
a. “A wireless communication client or extension unit comprising a plurality of memory, processors, programs, communication circuitry, authentication data stored on a subscribed identify module (SIM) card

and/or in memory and non-local calls database, at least one of the plurality of programs stored in the memory comprises instructions executable by at least one of the plurality of processors for”

78. *Andreini* discloses the preamble of claim 8. Or alternative, *Andreini* in view of *Walton* discloses the preamble of claim 8, to the extent the preamble is limiting. As shown in FIGS. 2 and 3 (reproduced below), *Andreini* discloses a peripheral device 13 (i.e., the “wireless communication client or extension unit” of claim 8) comprises: a memory unit 20 acting as a virtual SIM card (*Andreini* at ¶ 38) and a RAM unit 22 (*id.* at ¶ 41) (i.e., the “memory” of claim 8); CPU 16 (*id.* at ¶ 41) (i.e., the “processors” of claim 8); radio unit 17 (GSM1) equipped with a resident SIM card 19 and radio unit 18 (GSM2) connected to virtual SIM card 20 (*id.* at ¶¶ 37-38) (i.e., “communication circuitry” of claim 8); and “authentication parameters in the memory unit, 20” (*id.* at ¶ 41) (i.e., “authentication data stored on a subscribed identify module (SIM) card and/or in memory” of claim 8).



Foreign Wireless Communication Client or Extension Unit



90. *Andreini* discloses this element of claim 8. As shown in FIG. 3 (reproduced below), *Andreini* discloses peripheral devices 13 establishing “RAND variables” (*see id.* at ¶¶ 44-45) (i.e., “a local authentication information request” of claim 8) in response to a request for “the authentication procedure for that specific card” (i.e., “a local authentication request” of claim 8) by “the supplier which emitted the SIM card under verification” (*see id.* at ¶ 43) (i.e., “a local cellular communication network” of claim 8). *See id.* at ¶ 43 (“Once the calling has begun, module, 18, reads on the virtual card, 20, the parameters needed to start the authentication procedure; then it sends the access request, through the mobile telephony network, to *the supplier which emitted the SIM card under verification*; said supplier *launches the authentication procedure for that specific card by sending to module, 18, some variables, RAND*, which the SIM card under verification has to process according to a specific algorithm . . .”) (emphases added), ¶ 44 (“To do this, *CPU 16, transmits said variables, RAND*, through module, 17, to the central electronic unit, 14, which, as above said, houses the specific SIM card storing the above specific authentication algorithm”) (emphases added).

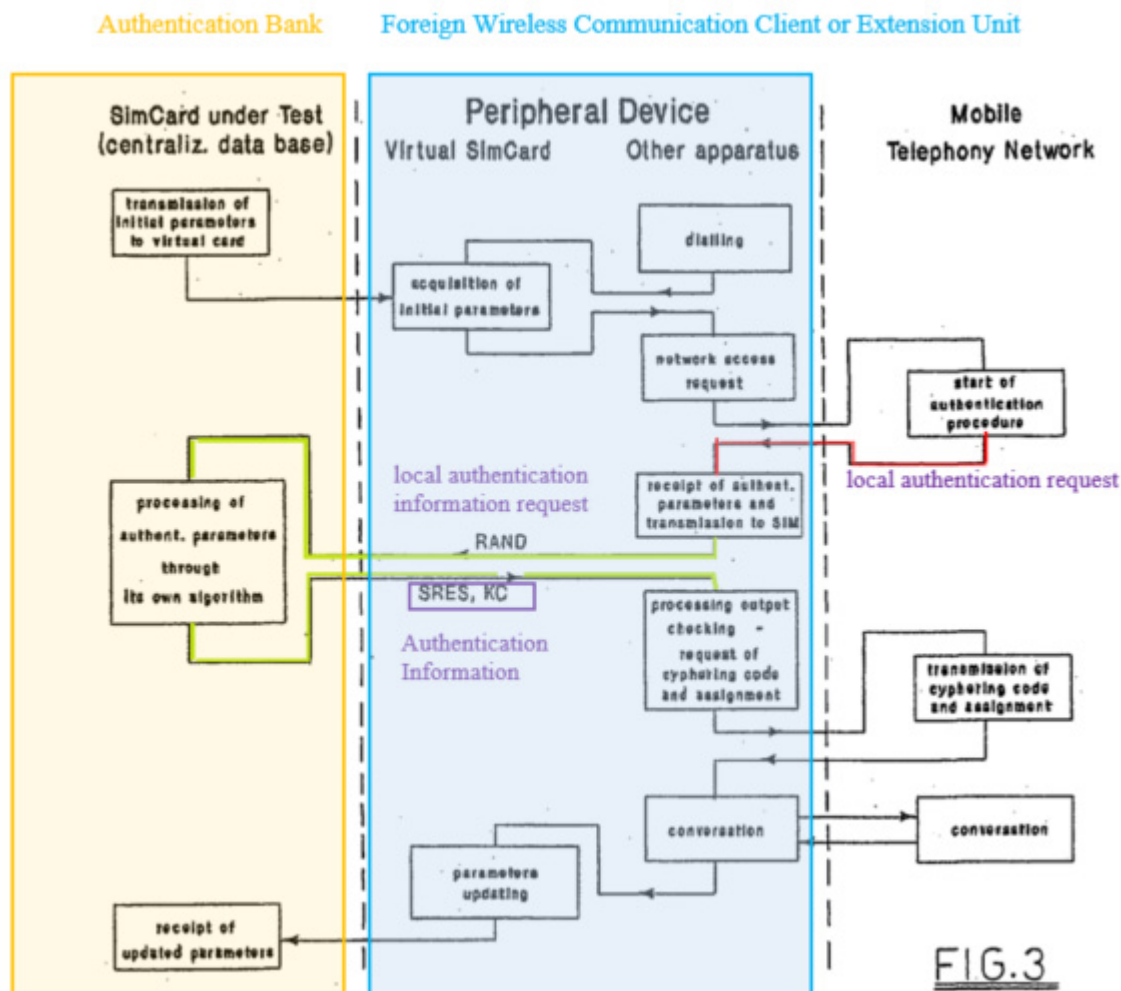


FIG.3

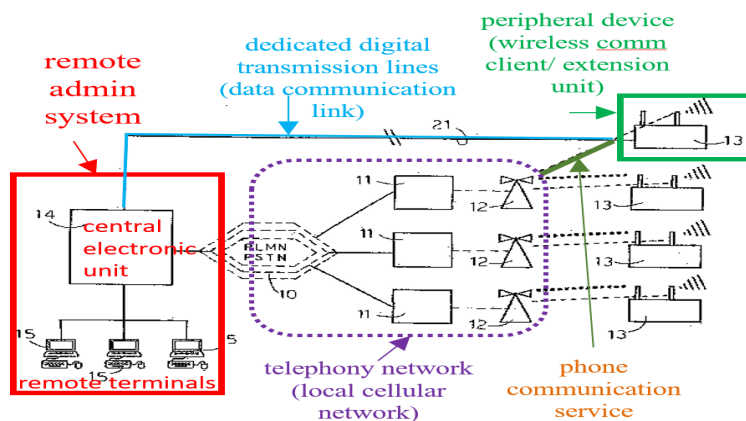
e. “wherein the local authentication information request comprises information regarding the local authentication request for local authentication information received by the foreign wireless communication client or the extension unit from the local cellular communication network”

91. *Andreini* discloses this element of claim 8. As shown in FIG. 3 above, *Andreini* discloses “RAND variables” (*see id.* at ¶¶ 44-45) (i.e., “the local authentication information request” of claim 8) comprises RAND regarding a request for “the authentication procedure for that specific card” (i.e., “a local authentication request” of claim 8) including “variables, RAND” received by peripheral devices 13 (i.e., “a foreign wireless communication client or an extension

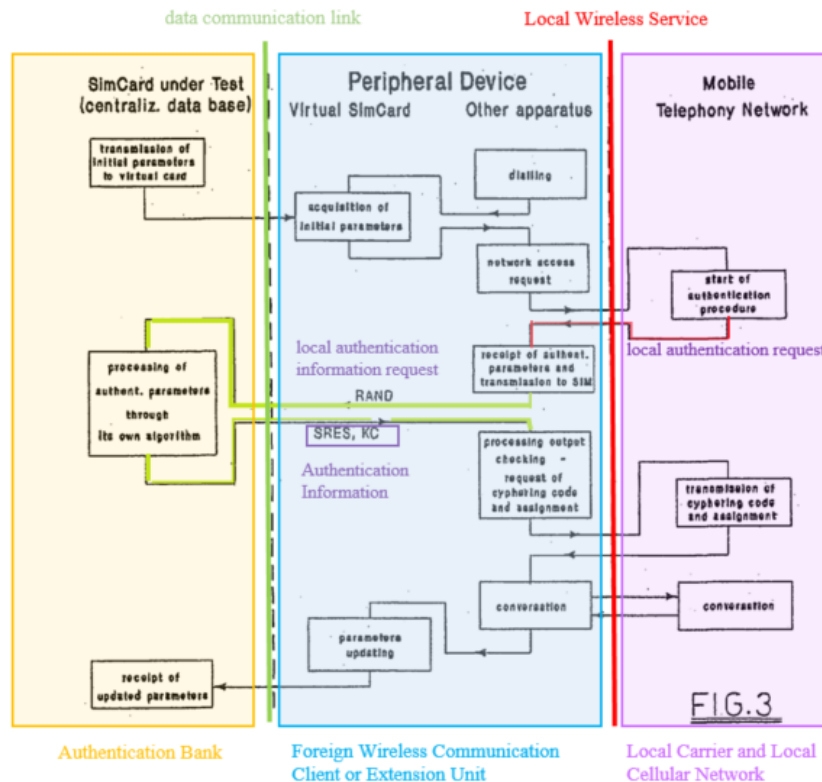
unit” of claim 8) from “the mobile telephony network” (*see id.* at ¶ 43) (i.e., “a local cellular communication network” of claim 8).

f. “and wherein the data communication link is distinct from the local cellular communication network”

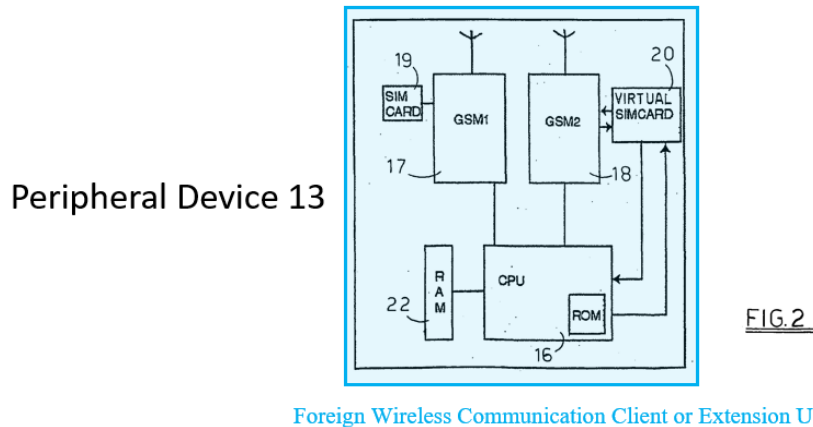
92. As illustrated in FIGS. 1 and 3 below, in *Andreini*, “[d]ata relating to verifications as well as said parameters are transmitted between peripheral devices and central electronic unit” either “through dedicated digital transmission lines” (i.e., “the data communication link” of claim 8) or “through the telephony network itself” (i.e., “the local cellular communication network” of claim 8). *Andreini* at Abstract; *see also id.* at ¶ 40. When the data transmitted through “dedicated digital transmission line” (i.e., the “communication link” of claim 8), the “dedicated digital transmission line” is evidently distinct from (i.e., not using) the “telephony network itself” (i.e., “the local cellular communication network” of claim 8), as is clearly shown in FIG. 1 below.



Andreini at FIG. 1



93. Furthermore, as shown FIG. 2 below, *Andreini* discloses that among radio module 17 (GMS1) and radio module 18 (GSM2) in the peripheral device 13 enables two distinct communication manners: “one unit apt to transmit and receive via radio” (i.e., the “local cellular communication network” of claim 8) and “one unit apt to transmit and receive through dedicated digital lines” (i.e., “data communication link” of claim 8). *Id.* at ¶ 28.



94. Therefore, in my opinion, *Andreini* discloses that the data communication link (e.g., the dedicated digital transmission line) is not using the local cellular communication network (e.g., the mobile telephony network).

g. “relaying the local authentication information request to the remote administration system via the data communication link and obtaining suitable local authentication information from the remote administration system via the data communication link”

95. *Andreini* discloses this element of claim 8. As shown in FIG. 3 above, *Andreini* discloses that the peripheral device 13 relays the variables RAND (i.e., the “local authentication information request” of claim 8) to the central electronic unit 14 (i.e., the “remote administration system” of claim 8) via the dedicated digital transmission line (i.e., “the data communication link” of claim 8). *See id.* at Abstract (“Data relating to verifications as well as said parameters are transmitted between peripheral devices and central electronic unit *through dedicated digital transmission lines* or through the telephony network itself.”) (emphasis added); *see also id.* at ¶ 40 (“the above data are transmitted to the CPU, 16, or *through dedicated digital lines, 21*, other through the mobile telephony network by using module, 17, equipped with its own SIM

card, 19.”) (emphasis added); *id.* at ¶ 44 (“CPU 16, transmits said variables, RAND, through module, 17, to the central electronic unit, 14 . . .”).

96. As illustrated in FIG. 3 above, *Andreini* further discloses obtaining a processing output consisted of “SRES parameter . . . [and] the KC (Key Cyphering) parameter” based on processing the RAND variables (i.e., the “suitable local authentication information” of claim 8) from the SIM card in central electronic unit 14 (i.e., the “remote administration system” of claim 8) via the dedicated digital transmission line (i.e., “the data communication link” of claim 8). *See id.* at ¶ 45 (“Once RAND variables have been processed, the processing output, consisted of SRES (Signature Response) parameter, is transmitted from SIM card under verification to module, 18...Together with said SRES parameter is also transmitted the KC (Key Cyphering) parameter.”); *see also id.* at Abstract (“Data relating to verifications as well as said parameters are transmitted between peripheral devices and central electronic unit *through dedicated digital transmission lines* or through the telephony network itself”) (emphasis added); *id.* at ¶¶ 40, 44.

97. To the extent that “relaying the local authentication information request to the remote administration system via the data communication link and obtaining **suitable** local authentication information from the remote administration system via the data communication link” of claim 8 (emphasis added) is limited to the specific embodiment disclosed in the ’689 patent at 17:67-18:14, 19:25-47, and 21:5-29, claim 8 is invalid for lack of enablement as discussed in Section X below.

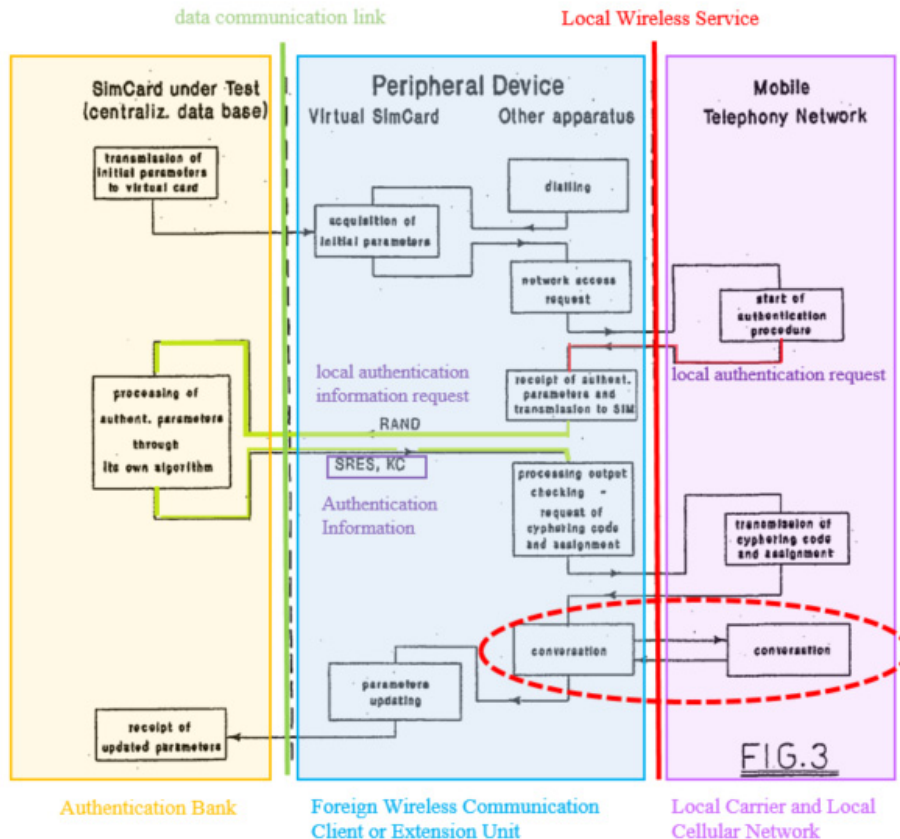
h. **“establishing local wireless services provided by the local cellular communication network to the wireless communication client or the extension unit by sending the local authentication information obtained from the remote administration system to the local cellular communication network over signal link; and”**

98. *Andreini* discloses this element of claim 8. In *Andreini*, after sending the authentication information (e.g., SRES parameter) to the mobile telephony network and getting verified, radio module 18 (GSM2) of peripheral device 13 (i.e., the “foreign wireless client or the extension unit” of claim 8) can now make phone call conversations via the mobile telephony network. *See Andreini* at ¶ 45, at FIG. 3. According to *Andreini*, “conversation represents the required type of **phone communication** among the available kinds of transmissions and **services.**” *Id.* at 45 (emphasis added).

99. Specifically, as shown in FIG. 3 (reproduced below), *Andreini* discloses establishing phone communications such as conversations (i.e., “local wireless services” of claim 8) provided by the mobile telephony network (i.e., “the local cellular communication network” of claim 8) to the peripheral device 13 (i.e., “the wireless communication client or the extension unit” of claim 8). *See id.* at ¶ 45 (“module 18, once the SRES parameter has been verified to be the right one, sends said KC parameter to the SIM card manager to get the code needed to *support the conversation*; note that, in this embodiment of the invention, *conversation represents the required type of phone communication* among the available kinds of transmissions and services.”) (emphases added); *see also id.* at claims 4 and 5 (“completing, by *said peripheral devices*, the verifications of the procedure to access the network said devices *acting*, upon reception of the above parameters, *as mobile telephones* containing the specific SIM cards whose parameters have been transmitted to them”) (emphases added).

100. In *Andreini*, phone communications (i.e., “local wireless services” of claim 8) is established by sending SRES parameter and the KC (Key Cyphering) parameter (i.e., “the local authentication information” of claim 8) from the SIM card in central electronic unit 14 (i.e., “the remote administration system” of claim 8) to the peripheral device 13 (i.e., the claimed “foreign

wireless communication client or the extension unit”) to the SIM card manager in the mobile telephony network (i.e., “the local cellular communication network” of claim 8) over signal link by module 18 (GSM2) of the peripheral device. *See Andreini* at ¶ 17 (“a second phase in which, during the verification, the remaining parameters [such as SRES parameter and the KC (Key Cyphering) parameter], needed to complete authentication and to ensure normal working of cards and devices, are transmitted” from the SIM card in central electronic unit 14 to the peripheral device 13); *id.* at 45 (“Once RAND variables have been processed, *the processing output, consisted of SRES (Signature Response) parameter, is transmitted from SIM card under verification to module, 18, still through the central electronic unit, 14, and through the auxiliary module, 17, which are to one another connected through the mobile telephony network.* Together with said SRES parameter is also transmitted the KC (Key Cyphering) parameter, since module 18, once the SRES parameter has been verified to be the [r]ight one, *sends said KC parameter to the SIM card manager to get the code needed to support the conversation*”); *see also id.* at ¶ 46 (“Finally, as last step before the conversation, *module 18, just like whichever mobile phone would do while regular[ly] working, asks to the service supplier, through the standard mobile telephony network, for the assignment, that is the right of managing the phone connection.*”) (emphasis added). Module 18 (GSM2) is a radio module communicating over a signal link of the mobile telephony network.



i. “providing a communication service to the wireless communication client or the extension unit according to the established local wireless services”

101. *Andreini* discloses this element of claim 8. Based on the established phone communication services (i.e., “the established local wireless services” of claim 8) to radio module 18 (GSM2), the peripheral device 13 (i.e., the “wireless communication client or the extension unit” of claim 8) is provided with a communication service (e.g., acting as mobile telephones). *Andreini* at ¶ 46 (“module 18...asks to the service supplier, through the standard mobile telephony network, for the assignment, that is the right of managing the phone connection.”); *see also id.* at claims 4 and 5, and ¶ 45.

152. *Patarkazishvili* discloses this element of claim 8. In *Patarkazishvili*, the communication terminal therefore receives a communication service of “route[ing] incoming and outgoing calls... to/from the cellular telephone network between terminal 201 and client computer 205” (*Patarkazishvili* at ¶ 41) to avoid high roaming billing rate while traveling away from home. *See* ¶ 29 (“embodiments of the present invention are intended to provide a system and method for making and receiving telephone calls while traveling or roaming away from home. The system and method avoid high roaming rates of cellular telephone networks.”). All mobile services are preferably available. *Id.* at ¶ 29. Also, other services such as “a phonebook, instant messages and short message service (SMS)” can be offered based on the established telephone communications (i.e., “the establishing local wireless services” of claim 8) to terminal 201.

153. Therefore, *Patarkazishvili* discloses providing a communication service (e.g., making and receiving telephone calls, optional services such as a phonebook, instant messages and short message service (SMS)) to the wireless communication client or the extension unit (e.g., communications terminal 201) according to the established local wireless services (e.g., telephone communications).

154. Therefore, *Patarkazishvili* discloses each and every element of claim 8, either expressly or inherently, and thus anticipates claim 8. Or alternatively, *Patarkazishvili* in view of *Walton* discloses, suggests, or teaches all elements of claim 8, and thus renders claim 8 obvious.

2. Claim 11

of *Walton* is to “provide a method for rerouting mobile phone communications, which involves least cost routing of the communications.” *Walton* at 3:15-20.

174. Second, *Patarkazishvili* discloses that “[t]he authentication information is required for authenticating the SIM module by the local cellular mobile telephone operator.” *Patarkazishvili* at ¶17. A PHOSITA would know that the aforesaid authentication information is not limited to a unique subscriber identifier. Accordingly, a PHOSITA would be motivated to look into other references like *Shi* and *Walton* to add some other common authentication information. It would be obvious for a PHOSITA to modify *Patarkazishvili* by adding the claimed “wireless communication client identifier, a password, and a current location of the foreign wireless communication client or the extension unit” as taught by *Shi* and *Walton* as authentication information. Such a modification could quickly and easily be achieved with predictable results, as it would merely require minor changes to *Patarkazishvili*.

175. Third, the number of authentication information is finite. It would be obvious for a PHOSITA to choose others like wireless communication client identifier, a password, and a current location of the foreign wireless communication client or the extension unit as authentication information from a finite number of identified, predictable items, with a reasonable expectation of success.

176. Thus, *Patarkazishvili* in view of *Shi* and *Walton* discloses all elements of claim 14, and thus renders claim 14 obvious.

E. *Kasper* in view of *Walton* Renders Claims 8 and 11-13 Obvious

177. As explained below, it is in my opinion that *Kasper* in view of *Walton* discloses all elements of claims 8 and 11-13, and thus renders these claims obvious.

1. Claim 8

a. **“A wireless communication client or extension unit comprising a plurality of memory, processors, programs, communication circuitry, authentication data stored on a subscriber identify module (SIM) card and/or in memory and non-local calls database, at least one of the plurality of programs stored in the memory comprises instructions executable by at least one of the plurality of processors for:”**

178. *Kasper* in view of *Walton* teaches the preamble of claim 8, to the extent the preamble is limiting. *Kasper* describes a mobile device/mobile station/GSM client (i.e., the “wireless communication client or extension unit” of claim 8). According to *Kasper*, the mobile device/mobile station/GSM client can be a mobile phone equipped with a SIM emulation adapter (*id.* at page 5, ¶ 5) and a hardware chip called MTM (mobile trusted module, *id.* at page 1, ¶ 1). The client therefore has a memory (e.g., non-volatile memory of MTM, *id.* at page 24, ¶ 2; page 28, ¶ 5), processors (e.g., secure co-processor, *id.* at page 37, ¶ 1), programs (e.g., trusted software layer of MTM, *id.* at page 37, ¶ 3), and communication circuitry (e.g., circuitry at least for establishing internet connection, *id.* at page 5, ¶ 5). In addition, the memory of MTM is capable of storing authentication data such as vSIM credential. *Id.* at page 78, ¶¶ 1-2 (“Protection of the vSIM Credential during execution... the secret individual key Ki would never leave the hardware protected environment of the MTM.”).

179. *Kasper* provides that its “model could be implemented in conventional GSM clients without any technological changes at the GSM infrastructure and at the GSM authentication protocol.” *Id.* at page 57, ¶ 1. Therefore, a PHOSITA would recognize that the GSM client in *Kasper*, corresponding to the “wireless communication client or extension unit” of claim 8, would at least have a voice call function, just like a conventional GSM phone would do. However, *Kasper* is silent on whether the GSM client has a non-local call database to facilitate its voice call function. But it is well known that at the time of the purported invention of ’689

patent (for example, February 2008), calls made by GSM phones to a local area and a non-local area are billed and charged differently.

180. The '689 patent described non-local calls database. For example, the '689 patent explained that “[t]he non-local calls database 525 lists **various locations, corresponding area codes**, and corresponding **local dial-in telephone numbers** for use when the subscriber wants to make a non-local call when present at a particular location.” Ex. 1001 at 15:55-60. The '689 patent further explains that “[w]hen a user desires to make a non-local call when within a particular location (e.g., a visiting caller in London wants to call his home office in San Francisco), the client 106 or extension unit 108 is able to determine that the called number is not within the local area, and then **dial a local communication server 128 (FIG. 1) at a local number from the list.**” *Id.* at 60-65. Therefore, the non-local calls database is a database comprising of information like various locations, corresponding area codes, and corresponding local dial-in telephone numbers, by which a non-local call is detected and the client or extension unit dials a local communication server at a local number from the database.

181. Likewise, *Walton* discloses a method “comprises means designed to detect when a call is being made by the GSM phone, to delay the GSM phone from making the call immediately, to send an IP message, containing the **Calling Line Identification (CLI)** corresponding to the calling GSM phone” (i.e. the “local dial-in telephone numbers” of the '689 patent), and “the **Dialed Number Identification (DNI)** corresponding to the correspondent phone line” (i.e., the “various locations, corresponding area codes” of the '689 patent) “**to a dedicated server**” (i.e., the “local communication server” of the '689 patent). *Walton* at 7:15-20.

182. Additionally, *Walton* discloses a local dial-in telephone number (e.g., the diverting number):

- (2) delay the GSM phone from making the call immediately,
- (3) send an IP message, containing the Calling Line Identification (CLI) corresponding to the calling GSM phone, and the Dialed Number Identification (DNI) corresponding to the Correspondent phone line, to the LCR Management Server,
- (4) have the LCR Management Server **send a diverting number** (of the Telecom witch) **to the GSM phone**.
- (5) have the GSM phone call **the diverting number** and the Telecom Switch receive the call;
- (6) have the Telecom Switch call the DNI sent in step (3) and connect the call.

Id. at 15:29-16:8 (emphases added). Whereas, the diverting number is a “local dial-in telephone number[]” of the ’689 patent.

183. Therefore, a PHOSITA would have been motivated to consider to have a non-local database on the GSM client of *Kasper* to use the non-local database to differentiate local and non-local calls so they can be billed and charged differently. One of such reference that a PHOSITA would have considered is *Walton*, which is also directed to a GSM Phone (i.e., wireless communication client) and a GSM Roaming Device (i.e., extension unit). According to *Walton*, the GSM Phone has memory (e.g., a MNC/MCC memory and a memory for storing a GSM Phone Application Software Program, *Walton* at 6:23-30), processors (e.g., processors including the one executing the GSM Phone Application Software Program, *id.* at 8:20-21), programs (e.g., programs including the GSM Phone Application Software Program, *id.* at 8:20-21), and communication circuitry (e.g., including at least the WPAN and WLAN chips, *id.* at

4:8-10). The GSM Phone in Walton additionally includes authentication data stored on a subscribed identify module (SIM) card (e.g., a SIM card that stores unique identity code, *id.* at 7:28-29, 2:27-34). *Walton* is designed for making outbound phone calls with least cost by rerouting mobile phone communications and particularly discloses the limitation of non-local calls database (e.g., Calling Line Identification (CLI), Dialed Number Identification (DNI), and diverting number). *See Walton* at 7:15-20.

184. In addition, a PHOSITA would have appreciated the similarity in approach of *Kasper* and *Walton*, which involve the way of requesting and providing authentication information of a SIM card. Same in both references, the SIM card used by a mobile device to authenticate itself in a local network is not inserted into or physically attached to the mobile device. Instead, the SIM cards are placed in a remote location and SIM data are transmitted over a wireless data connection. Both *Kasper* and *Walton* use such approach to eliminate the restriction of traditional physical SIM and provide a more flexible way for local mobile device to obtain authentication data that it needs.

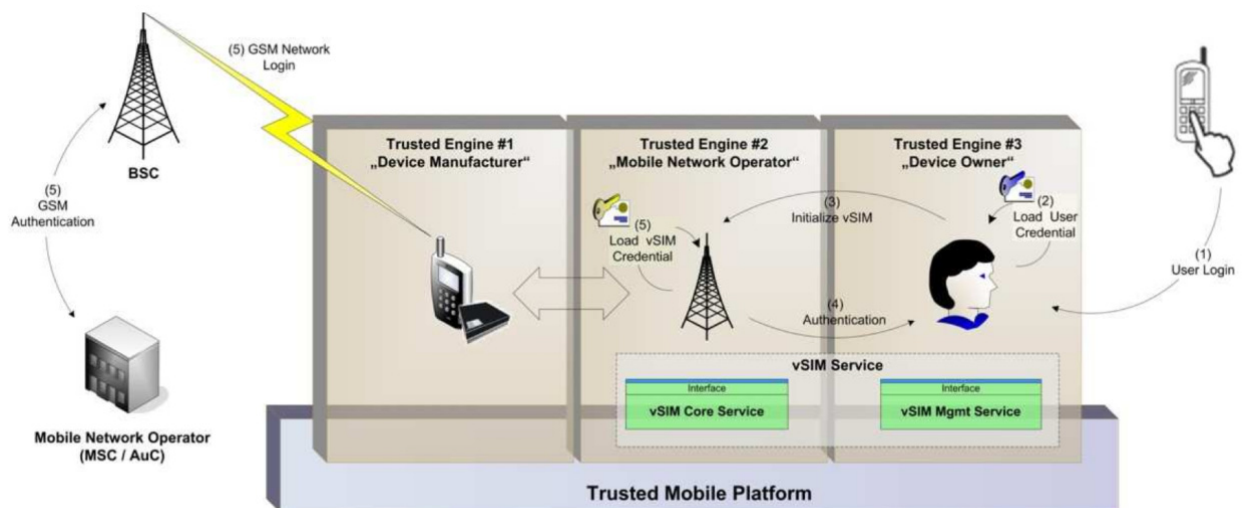
185. Therefore, a PHOSITA would have deemed it obvious to use the GSM phone or GSM roaming device of *Walton* to implement the GSM client of *Kasper*. In *Walton*, when the GSM Phone tries to make an outbound call or receive an incoming call, the system implements different methods of routing for local calls (*Walton* at 7:6-8 (“to fixed line or mobile numbers that are in the same local area of the mobile network corresponding to the virtual SIM”)) and non-local calls (*id.* at 7:9-11 (“other outbound calls”)). Therefore, the GSM phone has to contain a non-local calls database.

186. For all of these reasons, a PHOSITA would have been motivated to combine *Kasper* and *Walton* and deemed it obvious to implement the GSM client of *Kasper* in the same

way as GSM Phone or GSM Roaming Device of *Walton*, namely, implementing the GSM client of *Kasper* as having a non-local call database.

b. “enabling an initial setting of the wireless communication client or the extension unit and a remote administration system”

187. *Kasper* discloses this element of claim 8. *Kasper* discloses enabling an initial setting by “initialize[ing] the vSIM services and perform[ing] a log-in sequence”. *Kasper* at page 58, ¶ 1. The initial setting is conducted between a mobile device and a trusted subsystem TSSu of a Mobile Trusted Platform (MTP). The trusted subsystem TSSu “holds a vSIM_{MGMT} service” that is “responsible for administration and authentication of local users.” *Id.* at page 58, page 42, paras. 1-2. According to *Kasper*, “Once, the vSIMCORE has received the signed message, it verifies its status. Finally, the vSIMCORE unseals CredvSIM and initializes the SIM functionality using the IMSI_i and Ki (Step5).” *Id.* at page 59, ¶ 1. Such process is also illustrated as Step 1 through Step 5 in Figure 3.8 (reproduced below).



c. “establishing a data communication link to transmit information among the wireless communication client or the extension unit, and the remote administration system”

188. *Kasper* discloses this element of claim 8. *Kasper* also establishing a data communication link between the wireless communication client and the remote administration system. According to *Kasper*, “client uses an already established internet connection and connects to the central SIM server in order to relay the authentication messages.” *Kasper* at page 5, ¶ 5. More specifically, *Kasper* provides that such connection can be implemented as “existing PAN (e.g. Bluetooth) as well as an established connection to the destination device over the internet.” *Id.* at page 80, ¶ 2. To sum up, there is a data communication link (e.g., an internet connection or Bluetooth) connecting the wireless communication device (e.g., GSM client) and remote administration system (e.g., Central SIM server such as mobile trusted platform).

d. “establishing a local authentication information request in response to a local authentication request by a local cellular communication network, wherein the local authentication information request comprises information regarding the local authentication request for local authentication information received by the foreign wireless communication client or the extension unit from the local cellular communication network”

189. *Kasper* discloses this element of claim 8. *Kasper* discloses establishing a local authentication information request in response to a local authentication request by a local cellular communication network. In *Kasper*, the mobile device “requests for authentication at the GSM network” (*Kasper* at page 59, ¶ 4) and receives an authentication challenge $RAND_i$ from the GSM network (i.e., the “information regarding the local authentication request for local authentication information received by the foreign wireless communication client or the extension unit from the local cellular communication network” of claim 8). *Id.* at page 59, ¶ 4. $RAND_i$ is “information of identification and authentication of a subscriber” used by Authentication Center of GSM network. *Id.* page 11, ¶ 2. In response to $RAND_i$, the mobile

device establishes and relays an authentication message (i.e., the “local authentication information request” of claim 8) including at least the RAND_i to vSIM_{CORE} (i.e., “establishing a local authentication information request” of claim 8). *Id.* at page 59, ¶ 6 (“This RAND_i is passed to the trusted vSIM_{CORE} service.”), at page 5, ¶ 5 (“While performing network authentication, the client...connects to the central SIM server in order to relay the authentication messages”).

e. “and wherein the data communication link is distinct from the local cellular communication network”

190. *Kasper* discloses this element of claim 8. In *Kasper*, the data communication link between mobile device and the smart card server can be a Bluetooth connection or an established internet connection, which is distinct from local wireless services of the local carrier. *Kasper* at page 5, ¶ 5, and page 80, ¶ 4.

f. “relaying the local authentication information request to the remote administration system via the data communication link and obtaining suitable local authentication information from the remote administration system via the data communication link”

191. *Kasper* discloses this element of claim 8. *Kasper* discloses sending the authentication message including at least the RAND_i to vSIM_{CORE} (i.e., “relaying the local authentication information request to the remote administration system” of claim 8). *Id.* at page 59, ¶ 6 (“This RAND_i is passed to the trusted vSIM_{CORE} service.”), at page 5, ¶ 5 (“While performing network authentication, the client uses an already established internet connection and connects to the central SIM server in order to relay the authentication messages”). The message is relayed using the established internet connection (i.e., “the data communication link” of claim 8). *Id.* page 5, ¶ 5.

192. *Kasper* also discloses obtaining an authentication challenge response message SRES* from vSIM_{CORE} (i.e., “obtaining suitable local authentication information from the remote

administration system” of claim 8). *Id.* at page 59, ¶ 6 (“The output of the algorithm is the challenge response message SRES*. The vSIMCORE sends this SRES* message to the MNO.”), at page 5, ¶ 5 (“While performing network authentication, the client uses an already established internet connection and connects to the central SIM server in order to relay the authentication messages”). The response message is also obtained using the established internet connection (i.e., “the data communication link” of claim 8). *Id.* page 5, ¶ 5.

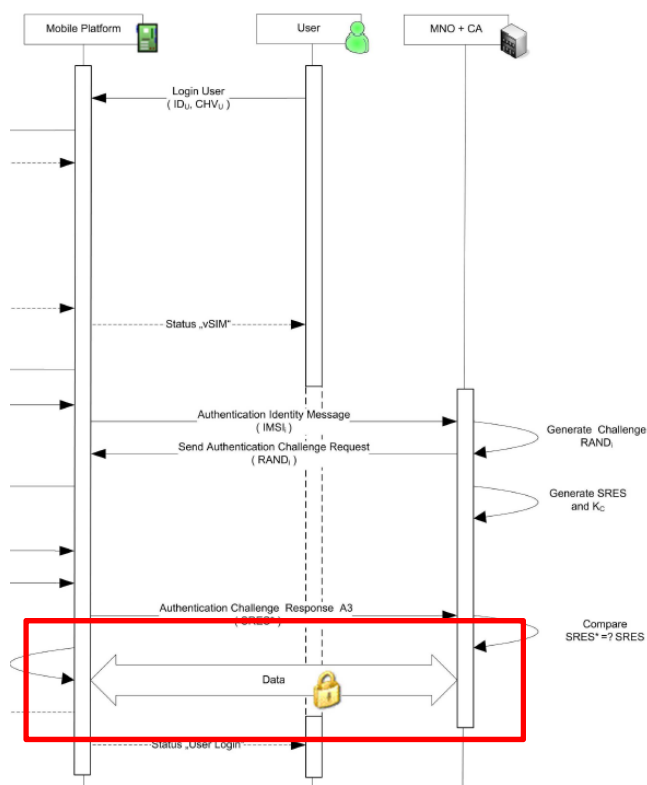
193. To the extent that “relaying the local authentication information request to the remote administration system via the data communication link and obtaining **suitable** local authentication information from the remote administration system via the data communication link” of claim 8 (emphasis added) is limited to the specific embodiment disclosed in the ’689 patent at 17:67-18:14, 19:25-47, and 21:5-29, claim 8 is invalid for lack of enablement as discussed in Section X below.

g. **“establishing local wireless services provided by the local cellular communication network to the wireless communication client or the extension unit by sending the local authentication information obtained from the remote administration system to the local cellular communication network over signal link;”**

194. *Kasper* discloses this element of claim 8. *Kasper* discloses establishing a local wireless service based on the obtained local authentication information. In *Kasper*, the mobile device relays the SRES* message as authentication information to the mobile network operator. After comparing it with the correct SRES, the mobile network operator confirms that “the subscriber is authenticated” and “enables subscriber access to mobile cellular networks” (i.e., local wireless services). *Kasper* at page 59, paras. 6-7, page 39, ¶ 2 (“we present a authentication model that is straight-forward to actual GSM standard and enables subscriber access to mobile cellular networks . . .”), and Figure 3.9.

h. “and providing a communication service to the wireless communication client or the extension unit according to the established local wireless services.”

195. *Kasper* discloses this element of claim 8. Based on “access to mobile cellular networks” (i.e., local wireless services), the mobile device in *Kasper* is provided with communication service. For example, the data service provided to mobile device by mobile network operator as illustrated in Figure 3.9 (partially reproduced below, markups added).



196. Thus, *Kasper* in view of *Walton* teaches all elements of claim 8, and thus renders claim 8 obvious.

2. Claim 11

a. “The wireless communication client or extension unit of claim 8, the memory comprising instructions executable by at least one of the one or more processors for”

197. Claim 11 depends from claim 8 and incorporates all limitations of claim 8, all of which are disclosed, suggested, or taught by *Kasper* in view of *Walton* as explained above in Section IX.E.1.

b. “relaying verification information to the remote administration system, wherein the verification information identifies the wireless communication client or extension unit as being associated with a user account of the remote administration system”

198. *Kasper* discloses this element of claim 11. For example, *Kasper* discloses relaying verification information to the mobile trusted platform. According to *Kasper*, during “Initialization of vSIM Credentials,” the user sends “a unique id ID_U with a proper password CHV_U to the vSIM_{MGMT} service” (i.e., “relaying verification information to the remote administration system” of claim 11). *Kasper* at page 58, ¶ 1.

199. The vSIM_{MGMT} then requests for vSIM credential initialization to the vSIM_{CORE} service and the vSIM_{CORE} service verifies the signature keys held by the vSIM_{MGMT} in order to authenticate the user identity. *Id.* at page 58, ¶ 2. If it is verified, the vSIM_{CORE} unseals the vSIM credential. *Id.* at page 59, ¶ 1. According to *Kasper*, “[a] vSIM credential CredvSIM is an identity-based identifier that can be used to authenticate a subscriber.” *Id.* at page 67, ¶ 3. Therefore, *Kasper* discloses identifying the user being associated with a user account (e.g., vSIM credential initialization).

200. A PHOSITA would be motivated to combine *Kasper* with *Walton* for the same reasons as that set forth in Section IX.E.1. Thus, *Kasper* in view of *Walton* teaches all elements of claim 11, and thus renders claim 11 obvious.

3. Claim 12

201. Claim 12 depends from claim 8 and incorporates all limitations of claim 8, all of

which are disclosed, suggested, or taught by *Kasper* in view of *Walton* as explained above in Section IX.E.1.

202. *Walton* further teaches the additional limitation **“the wireless communication client or the extension unit comprises a foreign wireless communication device not subscribed to the local network”** recited in claim 12. *Walton* provides GSM phone and GSM Roaming Device moving to a “changed network and/or country” (i.e., “not subscribed to the local network” of claim 12). *Walton* at 8:28-9:6 (“...upon detection of a change (which means the phone is roaming), an IP-message with the changed network and/or country is sent . . .”). *Walton* also gives an example of a “GSM phone roam[ing] from The Netherlands to Germany” (i.e., “not subscribed to the local network” of claim 12). *Id.* at 12:31-13:11.

203. A PHOSITA would be motivated to combine *Kasper* with *Walton* for the same reasons as that set forth in Section IX.E.1. Thus, *Kasper* in view of *Walton* teaches all elements of claim 12, and thus renders claim 12 obvious.

4. Claim 13

204. Claim 13 depends from claim 8 and incorporates all limitations of claim 8, all of which are disclosed, suggested, or taught by *Kasper* in view of *Walton* as explained above in Section IX.E.1.

205. *Kasper* further discloses the additional limitation **“requesting access to a desired local wireless service by sending a request to the local cellular communication network over a signal link”** recited in claim 13. For example, *Kasper* discloses “the mobile device requests for authentication at the GSM network” (i.e., “requesting access to a desired local wireless service” of claim 13). *Kasper* at page 59, ¶ 4. More specifically, the mobile device relays the IMSI as a request from vSIM_{CORE} to the network operator (i.e., sending a request to the local cellular communication network). *Id.* at page 59, ¶ 4.

206. To the extent that the claim limitation “a desired local wireless service” of claim 13 is limited to a local wireless service selected based on costs, *Walton* discloses the selection of preferred service according to costs, where it is preferred to “reroute mobile phone voice and data communication based on the lowest cost mobile operator for local calls and data whether the user is within the home network/country or in a foreign network/country.” *Walton* at 3:21-24. Therefore, the “lowest cost mobile operator for local calls and data” corresponds to “a desired local wireless service” of claim 13.

207. A PHOSITA would be motivated to combine *Kasper* with *Walton* for the same reasons as that set forth in Section IX.E.1. Thus, *Kasper* in view of *Walton* teaches all elements of claim 13, and thus renders claim 13 obvious.

X. CLAIM 8 IS INVALID UNDER 35 U.S.C. 112


208. Claim 8 is further invalid because it lacks enablement under 35 U.S.C. § 112, first paragraph, in the '689 patent specification, to the extent that “relaying the local authentication information request to the remote administration system via the data communication link and obtaining **suitable** local authentication information from the remote administration system via the data communication link” of claim 8 is limited to the specific embodiment disclosed in the '689 patent at 17:67-18:14, 19:25-47, and 21:5-29.

209. The specification of the '689 patent provides the following description of “obtaining **suitable** local authentication information from the remote administration system” of claim 8:

If the subscriber (or wireless communication client) is verified, the authentication server 118 of the administration system 116 obtains

create or assist in the creation of certain demonstrative evidence (not created yet) to assist me in testifying.

Executed on January 14, 2019


Martin J. Feuerstein

CERTIFICATE OF SERVICE

I certify that counsel of record for Plaintiff were served with a copy of the foregoing Invalidity Expert Report of Martin J. Feuerstein with Appendices 1-11 via email on this 14th day of January, 2019.

/s/ Robert W. Busby

Robert W. Busby